In response to the Official Action mailed July 12, 2007, please amend the claims to read as follows.

1. (currently amended) In a data processing operation having stored data in a plurality of data files, a system for protecting said data files from unauthorized users comprising:

means for storing for each of said plurality of data files, a backup file inaccessible to user requests;

means for receiving user requests for access to data files;

means for determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files;

means responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

2-3. (cancelled).

4. (original) The data processing operation system of claim 1 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.

5. (currently amended) In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a system for protecting said network site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests;

means associated with a network site for receiving user requests for access to data files;

means at said network site for determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;

means at said network site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

6. (cancelled)

7. (currently amended) In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a system for protecting said open Web site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests;

means associated with an open Web site for receiving user requests for access to data files;

means at said open Web site for determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;

means at said open Web site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

8-9. (cancelled).

10. (currently amended) In a data processing operation having stored data in a plurality of data files, a method for protecting said data files from unauthorized users comprising:

storing for each of said plurality of data files, a backup file inaccessible to user requests;

receiving user requests for access to data files;

determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files;

destroying the requested data files responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

11-12. (cancelled).

13. (original) The data processing method of claim 10 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

14. (currently amended) In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a method for protecting said network site data files from unauthorized users comprising:

storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests;

receiving user requests for access to data files at a network site;

determining at said network site, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;

destroying the requested data files responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

15-16. (cancelled).

17. (currently amended) In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a method for protecting said open Web site data files from unauthorized users comprising:

storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests;

receiving user requests for access to data files at said open Web site;

determining, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files at said open Web site;

destroying the requested data files at said open Web site responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

18-19. (cancelled).

20. (original) The World Wide Web communication network method of claim 17 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

21-30. (cancelled).

31. (new) A computer readable medium having stored thereon a computer readable program for protecting data stored in a plurality of data files from unauthorized users, wherein the computer readable program when executed on a computer causes the computer to:

store for each of said plurality of data files, a backup file inaccessible to user requests;

receive user requests for access to data files;

determine, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files;

destroy the requested data files responsive to an initial determination that a request is unauthorized; and

reload a backup file for each destroyed file.

32. (new) The computer readable medium of claim 31, wherein in determining whether said user requests are unauthorized intrusions, the computer readable program causes the computer to:

determine whether a user access identification code has been denied; and

determine whether the user has copied the requested files.

33. (new) A computer readable medium having stored thereon a computer readable program for protecting, from unauthorized users, data stored in a plurality of data files at network sites accessible in response to requests from users at other sites in the network, wherein the computer readable program when executed on a computer causes the computer to:

store for each of said plurality of data files at said network sites, a backup file inaccessible to user requests;

receive user requests for access to data files at a network site;

determine at said network site, without accessing any of said backup files, whether said user requests are unauthorized intrusions into said requested data files;

destroy the requested data files responsive to an initial determination that a request is unauthorized; and

reload a backup file for each destroyed file.

34. (new) The computer readable medium of claim 33, wherein the network is the World wide Web and said network sites are Web sites.

35. (new) The computer readable medium of claim 34, wherein in determining whether said user requests are unauthorized intrusions, the computer readable program causes the computer to:

determine whether a user access identification code has been denied; and

determine whether a user has copied the requested files.